Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Public Knowledge and Open Technology Institute at New America Petition for Rulemaking and Request for Emergency Stay of Operation of Dedicated Short-Range Communications Service in the 5.850-5.925 GHz Band (5.9)	)	RM-11771
	)	
	)	
	)	
	)	

To: The Commission

OPPOSITION TO PETITION FOR RULEMAKING

Thomas C. Power
Senior Vice President and General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

Jackie McCarthy
Director, Regulatory Affairs

CTIA
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

August 24, 2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY

CTIA and its members view the safety and security of new automotive technology as critical to the success of the emerging connected car ecosystem and public safety. The Public Knowledge and Open Technology Institute Petition, however, is a woefully misguided effort to achieve those ends.

As an initial matter, agencies other than the FCC have the appropriate expertise and have actively addressed cybersecurity and privacy issues implicated by connected cars. In particular, the National Highway Traffic Safety Administration ("NHTSA") has extensively considered connected car cybersecurity and privacy issues through research, thought leadership, and policymaking initiatives. In addition, the Federal Trade Commission has authority over connected car manufacturers' privacy and data security practices, and has specifically considered these issues in the Internet of Things context. These agencies also have made clear they will continue their efforts with regard to automobile cybersecurity and privacy.

Further, consistent with the federal government's approach to cybersecurity and privacy, the automotive industry, working with NHTSA, is working to adopt a comprehensive approach to security, and recently established self-regulatory privacy principles. These efforts, rather than top-down regulation from the FCC, will best ensure that new vehicular communications technologies like dedicated short-range communications ("DSRC") protect drivers.

The FCC, however, has no legal authority to intervene in the automotive industry by imposing novel cybersecurity and privacy regulations. To establish such regulations, the Petition proposes (with no substantive discussion) an unprecedented expansion of Commission authority. This legally unsustainable view of Commission authority lacks a limiting principle and would extend far beyond connected car cybersecurity and privacy to a wish list of *any* issues related to *any* services and industries that use spectrum-based technologies.

Finally, there is no basis to prohibit commercial operation in the DSRC service, which would stifle existing and emerging uses of this spectrum band. A government mandate to effectively disconnect DSRC from commercial uses runs counter to today's networked reality and could stifle innovative and societally-beneficial uses of this spectrum.

For these reasons, CTIA urges the Commission to swiftly deny the Petition.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Public Knowledge and Open Technology Institute at New America Petition for Rulemaking and Request for Emergency Stay of Operation of Dedicated Short-Range Communications Service in the 5.850-5.925 GHz Band (5.9)	)	RM-11771

To: The Commission

OPPOSITION TO PETITION FOR RULEMAKING

CTIA[1] hereby responds to the petition for rulemaking and request for emergency stay ("Petition") of Public Knowledge and Open Technology Institute ("Petitioners") asking the Commission to adopt cybersecurity and privacy rules specific to certain vehicle-to-vehicle ("V2V") technology, the Dedicated Short-Range Communications ("DSRC") service in the 5.9 GHz band.[2] The Petition also seeks to prohibit commercial operations in the DSRC service.

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry. With members from wireless carriers and their suppliers to providers and manufacturers of wireless data services and products, the association brings together a dynamic group of companies that enable consumers to lead a 21st century connected life. CTIA members benefit from its vigorous advocacy at all levels of government for policies that foster the continued innovation, investment and economic impact of America's competitive and world-leading mobile ecosystem. The association also coordinates the industry's voluntary best practices and initiatives and convenes the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] Petition for Rulemaking and Request for the Emergency Stay of Operation of Dedicated Short-Range Communications Service in the 5.850-5.9925 GHz Band (5.9 GHz Band) of Public Knowledge and the Open Technology Institute at New America, RM-11771 (filed June 28, 2016) ("Petition"). To even be considered, Commission rules require that a request to stay the effectiveness of any Commission decision or order be filed as a separate pleading. *See* 47 C.F.R. § 1.44(e). The Commission has not waived that rule here and instead put the Petition on public notice as a petition for rulemaking. *See* Public Notice, *Consumer & Governmental Affairs Bureau Reference Information Center, Petition for Rulemaking Filed*, Report No. 3048 (July 25,

CTIA and its members view the safety and security of new automotive technology as critical to the success of the emerging connected car ecosystem and public safety. The Petition, however, is a woefully misguided effort to achieve those ends. In particular:

- Certain federal agencies – namely, the National Highway Transportation and Safety Administration ("NHTSA") and the Federal Trade Commission ("FTC") – have the appropriate expertise and have actively addressed cybersecurity and privacy issues implicated by connected cars.

- Consistent with the federal government's approach to cybersecurity and privacy, the automotive industry, working with NHTSA, is working to adopt a comprehensive approach to security, and recently established self-regulatory privacy principles.

- The FCC, however, has no legal authority to intervene in the automotive industry by imposing novel cybersecurity and privacy regulations. Petitioners even acknowledge that their proposal to map the Commission's telephony customer propriety network information ("CPNI") privacy and data security regime onto the DSRC service does not readily fit.[3] Nor should it, as neither Congress nor the Commission intended, or even could have imagined, applying the CPNI regime to the connected car industry.

- There is no basis to prohibit commercial operation in the DSRC service, which would stifle existing and emerging uses of this spectrum band.

Given these developments and the FCC's lack of authority to regulate in this space, FCC cybersecurity and privacy rules would be unlawful, inappropriate, and unnecessary.

Ultimately, the unprecedented expansion of Commission authority sought by the Petition must be understood for what it is. Under Petitioners' view, the Commission would enjoy virtually unbounded authority to address *any* issues related to *any* services and industries that rely on wireless technologies in some form. For this reason alone, the Petition should be rejected.

2016) ("Interested parties may file statements opposing or supporting the *Petition for Rulemaking* listed herein….") (emphasis added). Accordingly, the stay request should be dismissed and CTIA responds to the requested rulemaking only.

[3] Petition at 21 ("DSRC is not a Title II service, nor would the Commission's CPNI regulations precisely fit the information that DSRC licensees contemplate collecting.").

I. THE COMMISSION IS NOT THE PROPER VENUE TO CONSIDER AUTOMOTIVE CYBERSECURITY AND PRIVACY ISSUES.

A. Regulatory Agencies Other than the FCC Have Primary Responsibility and Expertise Regarding Automotive Technology Safety, Cybersecurity, and Privacy.

The federal government has sufficient existing oversight and recourse on issues of automotive cybersecurity and privacy. Indeed, NHTSA and the FTC *already have* considered – and can consider should they arise – automotive technology safety and privacy issues consistent with their respective authorities and expertise.

1. NHTSA Has Focused Extensively on Cybersecurity and Privacy Implications of V2V Technologies.

NHTSA and the Department of Transportation ("DOT") have considered the impact of V2V technologies on driver safety for nearly a decade.[4] DOT Secretary Anthony Foxx has explained that DOT "wants to speed the Nation toward an era when vehicle safety is not just about surviving crashes; it is about avoiding them."[5] To achieve this goal, NHTSA has recognized that "cybersecurity must be an integral part of vehicle engineering, manufacturing, and enforcement" and therefore "is laying the groundwork needed for the road ahead."[6]

---

[4] *See, e.g.*, NHTSA Vehicle Safety Rulemaking and Research Priority Plan 2009-2011, Docket No. NHTSA-2009-0108-0001 (rel. July 2009), http://www.nhtsa.gov/staticfiles/rulemaking/pdf/2009-2011_Rulemaking_and_Research_Priority_Plan.pdf; NHTSA Vehicle Safety and Fuel Economy Rulemaking and Research Priority Plan 2011-2013, Docket No. NHTSA-2009-0108-0032 (rel. Mar. 2011), http://www.nhtsa.gov/staticfiles/rulemaking/pdf/2011-2013_Vehicle_Safety-Fuel_Economy_Rulemaking-Research_Priority_Plan.pdf.

[5] *See* NHTSA, *NHTSA and Vehicle Cybersecurity*, http://www.nhtsa.gov/About+NHTSA/Speeches,+Press+Events+&+Testimonies/NHTSA+and+Vehicle+Cybersecurity (last accessed Aug. 24, 2016) ("*NHTSA Vehicle Cybersecurity*").

[6] *Id.*

In fact, over the last several years, NHTSA has been at the forefront of research, thought leadership, and policymaking efforts regarding connected car cybersecurity in particular, and connected car privacy as well. By way of example, NHTSA's initiatives include the following:

- Research and testing
    - The creation of a new research division to focus specifically on issues pertaining to vehicle electronics and cybersecurity.[7]
    - The expansion of research and testing capabilities at a test center to better evaluate "electronics reliability (including functional safety), automotive cybersecurity, [and] automated vehicles."[8]
    - Direct engagement with white-hat hackers to better understand and address connected car security issues.[9]
    - The establishment of partnerships with the Defense Advanced Research Projects Agency ("DARPA") to develop a secure reference parser for V2V communication interfaces based on DARPA's extensive research and experience and with other defense agencies and with the National Institute of Standards and Technology ("NIST") to leverage and share knowledge and expertise.[10]
    - A request for information to, among other things, identify private entities interested in developing components of a V2V Security Credential Management System.[11]

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] NHTSA, *Vehicle-to-Vehicle Security Credential Management System; Request for Information*, 79 Fed. Reg. 61927 (Oct. 15, 2014), https://www.gpo.gov/fdsys/pkg/FR-2014-10-15/pdf/2014-24482.pdf.

- Thought leadership including through the release of four separate cybersecurity reports[12]

    - *Characterization of Potential Security Threats in Modern Automobiles.* A report describing "a composite modeling approach for potential cybersecurity threats in modern vehicles," including both cyber threat use case examples and completed threat matrices.[13]

    - *NIST Cybersecurity Risk Management Framework Applied to Modern Vehicles*. A report, building on the NIST Cybersecurity Framework, to serve "as a primer that establishes a baseline conceptual understanding of the NIST approach … and a common vocabulary for discussing risk management for the automotive sector."[14]

    - *A Summary of Cybersecurity Best Practices*. A review of cybersecurity best practices involving electronic control systems across a variety of industry segments, "provid[ing] relevant benchmarks that are informative to making strategic decisions for NHTSA's research program."[15]

    - *Assessment of the Information Sharing and Analysis Center Model.* An assessment of the cybersecurity information sharing forum model known as an Information Sharing and Analysis Center ("ISAC") and the implementation of an ISAC for the automotive sector (the "Auto ISAC").[16]

---

[12] These reports together "increase the collective knowledge base in automotive cybersecurity; help identify potential knowledge gaps; help describe the risk and threat environments; and help support follow-on tasks that could be used to establish security guidelines." NHTSA, *A Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach*, at iii (Oct. 2014), http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812074_Characterization_PotentialThreatsAutos(1).pdf.

[13] *Id.* at iii, Appendices A & B.

[14] NHTSA, *National Institute of Standards and Technology (NIST) Cybersecurity*

Risk Management Framework Applied to Modern Vehicles, at ii (Oct. 2014), http://www.nht http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812073_NatlInstitStandardsTechCyber.pdf.

[15] NHTSA, *A Summary of Cybersecurity Best Practices*, at ii-iii (Oct. 2014), http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812075_CybersecurityBestPractices.pdf.

[16] NHTSA, *Assessment of the Information Sharing and Analysis Center Model* (Oct. 2014), http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812076-AssessInfoSharingModel.pdf. As described below, the industry since has established an Auto ISAC.

- Policymaking

    - The inclusion of cybersecurity and privacy issues as part of a broader ongoing rulemaking with DOT on performance requirements for V2V devices and messages for passenger cars and light truck vehicles, that seeks information on whether a V2V system creates new potential threat vectors into vehicles and how NHTSA could mitigate any potential threats.[17]

    - Beyond the agency's own policymaking, the development of a legislative proposal with DOT that, according to NHTSA, could "*further* improve the cybersecurity posture of vehicles," including by establishing liability for hackers.[18]

Beyond these myriad efforts, NHTSA included extensive discussion of both cybersecurity and privacy issues in its comprehensive report on V2V technologies. With regard to V2V communications security, the NHTSA V2V report dedicates 50 pages to a discussion of a security design concept and other security issues.[19] NHTSA stated that it "would perform its traditional regulatory role," *i.e.*, ensuring compliance with any established safety standards.[20]

With regard to privacy, NHTSA stated that in any initiative to regulate V2V technologies, it was "committed to doing so in a manner that both protects individual privacy and promotes this important safety technology."[21] NHTSA further established the following:

> [T]he V2V system as contemplated by NHTSA … will not collect or store any data on individuals or individual vehicles, nor will it enable the government to do so. There is no data in the safety messages exchanged by vehicles or collected by the V2V security system that could be used by law enforcement or private entities to

[17] NHTSA, *Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications*, Advance Notice of Proposed Rulemaking, 79 Fed. Reg. 49270 (Aug. 20, 2014), http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/V2V-ANPRM_081514.pdf.

[18] *NHTSA Vehicle Cybersecurity* (emphasis added).

[19] NHTSA, *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application V2V Report*, at 158-95 (Aug. 2014), http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf ("*NHTSA V2V Report*").

[20] *Id.* at 195.

[21] *Id.* at 147.

> personally identify a speeding or erratic driver. The system—operated by private entities—will not permit tracking through space or time of vehicles linked to specific owners or drivers…. The system will not provide a 'pipe' into the vehicle for extracting data.[22]

Moreover, NHTSA stated it would "continue to work with [DOT's] Privacy Officer and Office of the General Counsel to assess and reassess any threats to privacy that may be introduced by V2V technology and help identify mitigation measures to minimize any such risks."[23]

Notably, the NHTSA initiatives listed above, complemented by the industry's proactive measures, will culminate soon in cybersecurity guidance that reflects the agency's thinking on this issue, its collaboration with both the automotive and communications industries, and its subject matter expertise on vehicle technical and safety issues. Suffice to say, in contrast to the Petition's suggestions otherwise, NHTSA has extensively considered cybersecurity and privacy issues associated with V2V technology and has made clear its intention to continue to do so.

2. The FTC Has Authority Over Automakers' Privacy and Data Security Practices.

The FTC also maintains authority over automakers. Because they are not common carriers, automakers are subject to FTC enforcement should they undertake deceptive or unfair privacy and data security practices.[24] There is no reason why the FTC cannot exercise its authority to address privacy and data security concerns related to connected cars and V2V technologies, should they arise.

Perhaps tellingly, the Petition does not acknowledge the FTC's privacy and data security expertise (other than a passing reference to past coordinated efforts between the FCC and

---

[22] *Id.* at 144.

[23] *Id.* at 148.

[24] *See* 15 U.S.C. § 45.

FTC).[25] The FTC, however, has created a successful government approach to privacy that protects online consumers' personal information through its flexible notice-and-choice framework, and through the threat of enforcement as a backstop to ensure that companies in the ecosystem implement and adhere to their privacy promises. As CTIA has previously noted, the FTC's approach is the gold standard for establishing a coherent, cross-sectoral approach to protecting consumer privacy.[26]

In addition to the FTC's expansive cross-industry privacy and data security expertise, the agency also has specifically examined connected car issues. As part of its 2013 Internet of Things ("IoT") workshop, the FTC held a panel that examined the benefits and risks of connected cars, including significant discussion of privacy and security concerns.[27] A follow-up report on the IoT workshop reflected the FTC's intent to use enforcement and its consumer and business education tools to ensure that IoT companies, including connected car manufacturers, account for security and privacy issues as they develop new devices.[28] The report specifically stated that the FTC "will continue to look for cases involving companies making IoT devices that, among other things, do not maintain reasonable security, make representations about their

[25] *See* Petition at 10.

[26] *See* Comments of CTIA, WC Docket No. 16-106, at 5 (filed May 26, 2016).

[27] FTC, *FTC Announces Agenda, Panelists for Upcoming Internet of Things Workshop* (Nov. 8, 2013), https://www.ftc.gov/news-events/press-releases/2013/11/ftc-announces-agenda-panelists-upcoming-internet-things-workshop; FTC, *Internet of Things Workshop* (Nov. 19, 2013), https://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf; FTC, *The Internet of Things: Privacy & Security in a Connected World*, at 3-4 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf ("*FTC IoT Report*").

[28] *FTC IoT Report* at viii-ix, 53.

privacy practices, or violate the requirements of the [Fair Credit Reporting Act]…."[29] In other words, the FTC will act where security and privacy issues arise in IoT applications, including with respect to connected cars.

More recently, the FTC has directly addressed connected car issues. As part of the NHTSA V2V proceeding, the FTC discussed its own authority and activity in the privacy and data security area and described security and privacy issues raised during its IoT workshop.[30] The FTC also commended NHTSA for taking into account privacy and security concerns, and expressed support for "NHTSA's implementation of a deliberative, process-based approach to address privacy and security risks."[31] Subsequently, during a connected car conference this past February, FTC Commissioner Terrell McSweeny explained the FTC's role in ensuring the safety, security, and privacy of connected cars as follows:

> [Consumers] should be able to have a reasonable expectation that if they purchase a product or a service, the personal information they provide will be protected. The same principle applies to the Internet connected devices, the web services, and mobile applications they use, and the connected cars they drive.[32]

---

[29] *Id.* at 53. The report also offered recommendations for companies developing IoT products and services, including by providing operating system and software updates to ensure ongoing protection from evolving data security and privacy threats. *See id.* at 31.

[30] Comment of the FTC to Advance Notice of Proposed Rulemaking Regarding Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications Pursuant to Chapter 301 of the Department of Transportation Motor Vehicles and Driver Programs, Docket No. NHTSA-2014-0022, at 2-6 (filed Oct. 20, 2014), https://www.ftc.gov/system/files/documents/advocacy_documents/federal-trade-commission-comment-national-highway-traffic-safety-administration-regarding-nhtsa/141020nhtsa-2014-0022.pdf.

[31] *Id.* at 6.

[32] Terrell McSweeny, Cmm'r, FTC, Keynote Remarks at Connected Cars USA 2016, at 2 (Feb. 4, 2016), https://www.ftc.gov/system/files/documents/public_statements/913813/mcsweeny_-_connected_cars_usa_2016_2-4-16.pdf ("McSweeny Connected Car Remarks"); *see also* Edith Ramirez, Chairwoman, FTC, Remarks at International Conference on Big Data from a Privacy Perspective, at 5, 8 (Jun. 10, 2015),

Put simply, the FTC has authority, expertise, and a substantial role in ensuring that connected cars and V2V technologies do not compromise drivers' safety, information security, and privacy.

In sum, taking into account NHTSA and FTC oversight, there is no gap that the FCC needs to address.

B. Existing Frameworks Are Addressing Connected Car Cybersecurity and Privacy Concerns.

In addition to the work of NHTSA and the FTC, the automotive industry is proactively addressing cybersecurity and privacy issues in a manner consistent with the Administration's endorsement of industry-led, self-regulatory models.

1. The Automotive Industry Is Addressing Cybersecurity Issues Consistent with the Administration's Cybersecurity Framework.

The prevailing approach to cybersecurity has been to rely on voluntary models that give companies the flexibility to improve security and user trust in an environment where risks are constantly evolving and different industry segments (and even individual companies) have unique needs. That approach reflects a deliberate and reasoned choice, and originates in this Administration's Executive Order directing the development of an industry-led, voluntary, risk- and outcome-based cybersecurity framework rather than a prescriptive compliance regime.[33] The response to that mandate – the NIST Cybersecurity Framework[34] – "is not a one-size-fits-all

---

https://www.ftc.gov/system/files/documents/public_statements/671661/150610era_bigdata.pdf (noting privacy and security issues associated with connected cars).

[33] Exec. Order 13636, *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 11739, 11740-41 (Feb. 19, 2013), https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (creating a "voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and other interested entities" and directing that the framework be "flexible, repeatable, performance-based, and cost-effective" and "incorporate voluntary consensus standards and industry best practices to the fullest extent possible").

[34] Nat'l Inst. of Standards & Tech. (NIST), *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (Feb. 12, 2014) ("*NIST Cybersecurity Framework*").

approach to managing cybersecurity risk" but instead "is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes."[35] The automotive industry work on cybersecurity reflects this approach.[36] The Petition does not.

Notably, the Petition does not even mention the NIST Cybersecurity Framework. This silence should not be surprising, as the Petition's call to impose specific rules on a particular technology is wholly incompatible with the NIST Cybersecurity Framework and the paradigm the Commission supports. Rather than abruptly changing course by launching an ill-advised rulemaking, the Commission should stay true to its current direction and continue to foster industry-led solutions.

While cybersecurity vulnerabilities present novel challenges to automotive safety, they also require new approaches to address them.[37] Automotive industry initiatives, including industry information-sharing and other collaborative initiatives are a key part of any solution. Indeed, with NHTSA's encouragement, the automotive industry voluntarily developed and launched the Auto ISAC in September 2015 to enable and promote the exchange of significant

---

[35] *NIST Cybersecurity Framework* at 2, 6.

[36] The FCC itself has embraced this philosophy. Just last week, Chairman Wheeler emphasized the Commission's intent to continue building on the NIST Cybersecurity Framework where "industry and the FCC work together to develop standards and processes" and "the FCC does not impose specific regulations[.]" Tom Wheeler, Chairman, FCC, Remarks at Aspen Institute 2016 Communications Policy Conference, at 5 (Aug. 14, 2016), http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0815/DOC-340777A1.pdf.

[37] As NHTSA has correctly recognized, because of the "highly-dynamic nature of cybersecurity risks and threats," performance standards are "difficult to set without the risk of becoming outdated quickly." NHTSA & DOT, *Electronic Systems Performance in Passenger Motor Vehicles* 47 (Dec. 2015), http://www.nhtsa.gov/staticfiles/laws_regs/pdf/Electronic-Systems-Performance-in-Motor%20Vehicles.pdf.

threat information, and countermeasures, in real time.[38] More recently, the Auto ISAC has released a set of automotive cybersecurity best practices, and now is working on the development of supplemental materials.[39] Finally, automakers are also establishing partnerships with third parties, including the wireless industry, security technologists, non-profits, government programs, and others to develop vehicle-specific security technologies and practices.[40] As noted above, NHTSA, building on these industry-led initiatives, is expected to soon issue cybersecurity guidance.

Contrary to the Petition's alarmism, relevant agencies and industry are working to address V2V cybersecurity concerns. These efforts, rather than ill-advised regulation from the FCC, will best ensure the cybersecurity of new vehicular technologies like DSRC.

2. The Automotive Industry Is Proactively Addressing Privacy Concerns.

The automotive industry's privacy efforts complement its cybersecurity efforts. In 2014, the industry voluntarily adopted consumer privacy protection principles (the "Principles"), which apply to new vehicles manufactured no later than the 2017 model year and for vehicle technologies and services subscriptions begun or renewed after January 2, 2016.[41] The Principles establish a framework based on the Fair Information Practice Principles that

[38] NHTSA has described the Auto ISAC as "a critical piece of vehicle cybersecurity infrastructure, as manufacturers and suppliers are in the best position to identify weaknesses in their own products." *NHTSA Vehicle Cybersecurity*.

[39] *See* Auto ISAC, *Automotive Cybersecurity Best Practices: Executive Summary* (Jul. 2016), http://www.automotiveisac.com/best-practices/.

[40] *See* Auto Alliance, *Cybersecurity: An Industry-wide Effort to Identify Emerging Threats and Potential Adversaries*, http://www.autoalliance.org/auto-issues/cybersecurity (last accessed Aug. 24, 2016) (listing industry activities and partnerships).

[41] Auto Alliance, *Automotive Privacy: Automakers believe that strong consumer data privacy protections are essential to maintaining the trust of our customers*, http://www.autoalliance.org/auto-issues/automotive-privacy/automotive-privacy (last accessed Aug. 24, 2016).

automakers and other participants in the automotive industry can adopt.[42] The framework specifically establishes the following principles for the connected car context: transparency; choice; respect for context; data minimization, de-identification, and retention; data security; integrity and access; and accountability.[43] The Principles establish accountability: As FTC Commissioner Terrell McSweeny has noted in reference specifically to the Principles, "[t]he FTC takes seriously our responsibility in helping signatories adhere to industry best practices."[44]

This voluntary, self-regulatory approach is consistent with the Administration's Consumer Privacy Bill of Rights. As the Administration has recognized, "afford[ing] companies discretion in how they implement" privacy principles "promote[s] innovation" and "encourage[s] effective privacy protections" as companies can address "privacy issues that are likely to be most important to their customers and users, rather than requiring companies to adhere to a single rigid set of requirements."[45] In contrast, "adopting legal requirements that prescribe specific technical requirements … could … inhibit innovation."[46] The Petition seeks to involve the FCC and would do just what the Administration argues against: imposing prescriptive regulation and inhibiting innovation of critical V2V communications technologies and applications.

---

[42] Auto Alliance, *Auto Issues*, http://www.autoalliance.org/auto-issues/automotive-privacy/principles (last accessed Aug. 24, 2016).

[43] *See id.; see also* Letter from the Auto Alliance and Global Automakers to the FTC (Nov. 12, 2014), http://www.autoalliance.org/auto-issues/automotive-privacy/letter-to-the-ftc.

[44] McSweeny Connected Car Remarks at 4.

[45] The White House, *Consumer Data Privacy in a Networked World*, at 2 (Feb. 2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[46] *Id.* at 24; *see also FTC IoT Report* at 48-49 (self-regulatory programs designed for particular industries would be helpful to encourage the adoption of privacy- and security-sensitive practices).

C. The FCC Has No Legal Authority to Impose DSRC Cybersecurity and Privacy Requirements.

With NHTSA, the FTC, and the industry actively addressing cybersecurity and privacy concerns associated with connected cars, FCC intervention is entirely unwarranted – and, as discussed here, unlawful.

The Petition's lack of any substantive discussion of FCC legal authority to impose DSRC cybersecurity and privacy requirements is striking. It calls for Section 222-like obligations on DSRC but acknowledges that "DSRC is not a Title II service, nor would the Commission's CPNI regulations precisely fit the information that DSRC licensees contemplate collecting."[47] As a legal matter, it is insufficient to make a single passing reference to provisions in Section 303 and conclude that "no one can doubt that protecting the privacy and security of America's drivers serves 'the public interest, convenience and necessity.'"[48] These provisions – Sections 303(r) and 303(b) – do not provide any basis for the FCC to adopt DSRC cybersecurity and privacy requirements.

Section 303(r) enables the Commission to "[m]ake such rules and regulations . . . as may be necessary to carry out the provisions of the Communications Act."[49] While this section provides procedural rulemaking authority to the Commission, the Commission may not rely on this section "without mooring its action to a distinct grant of authority in [Title III]."[50] Section

---

[47] Petition at 21.

[48] *Id.* at xii-ix.

[49] 47 U.S.C. § 303(r).

[50] *Cellco P'ship v. FCC*, 700 F.3d 534, 542 (D.C. Cir. 2012) ("*Cellco*"), *citing Motion Picture Ass'n of Am., Inc. v. FCC*, 309 F.3d 796, 806 (D.C. Cir. 2002) ("*MPAA*").

303(r) itself "confers no independent authority."[51] Rules adopted under Section 303(r) are "justified only if the FCC had authority to act pursuant" to some other provision of the Act:[52]

> The FCC cannot act in the "public interest" if the agency does not otherwise have the authority to promulgate the regulations at issue. An action in the public interest is not necessarily taken to "carry out the provisions of the Act," nor is it necessarily authorized by the Act. The FCC must act pursuant to *delegated authority* before any 'public interest' inquiry is made under § 303(r).[53]

But the Petition does not, nor can it, show that automotive industry cybersecurity and privacy rules are "necessary" to carry out any substantive authority set forth in the Communications Act.

Given the absence of independent authority under Section 303(r), the Petition rests solely on the relatively narrow scope of substantive authority delegated under Section 303(b). That section gives the Commission authority to "[p]rescribe the nature of the service to be rendered by each class of licensed [radio] stations and each station within any class."[54] By its plain language, this provision does not authorize adoption of DSRC cybersecurity and privacy rules. Only rules that "merely define[] the form" of radio services for those who seek a license to offer them fall within Section 303(b)'s ambit.[55] For example, the D.C. Circuit has held that Section 303(b) provided authority for the Commission to adopt its data roaming rules.[56] By requiring a mobile data licensee to offer other licensees access to its wireless network, these rules – per the court – define the form of the wireless service offered by the licensee. By contrast, cybersecurity and privacy rules applied to DSRC licensees would not "define[] the form" of DSRC, but would

---

[51] *Id.*, *citing MPAA*, 309 F.3d at 806.

[52] *MPAA* at 806.

[53] *Id.*

[54] 47 U.S.C. § 303(b).

[55] *See Cellco*, 700 F.3d at 543 (upholding the FCC's data roaming rule, which "merely define[d] the form mobile-internet service must take for those who seek a license to offer it").

[56] *See id.*

instead regulate the business practices of automakers simply because those parties happen to use DSRC in the conduct of their business.

The unprecedented expansion of Commission authority sought by the Petition must be understood for what it is. Under Petitioners' view of these Section 303 provisions, the Commission's authority would extend far beyond connected car cybersecurity and privacy to a wish list of *any* issues related to *any* services and industries that use wireless technologies. There is neither a "sector-specific" limiting principle, nor any limiting principle whatsoever. Regulation under Petitioners' view could expand beyond cybersecurity and privacy and to any number of businesses and industries that rely on wireless connectivity in some form, including, but not limited to, retailers that accept mobile payments, taxicabs and first responders that use radio dispatch, healthcare companies that offer wireless-based health and wellness solutions, manufacturers of "smart home" devices, local jurisdictions that deploy "smart city" architecture, automated industrial plant owners, and utilities that use spectrum for smart grid applications. Under Petitioners' reasoning, this expanded jurisdiction would presumably extend to licensed *and* unlicensed services because, while Section 303(b) is limited to licensees, Section 303(r) is not. Although unlimited FCC jurisdiction over spectrum-based services may be the result that Petitioners seek, it is wholly unauthorized by the Commission's enabling statute and would amount to an unbounded expansion of authority. For this reason alone, the Petition should be rejected.

II. THE COMMISSION SHOULD NOT LIMIT DSRC TO NON-COMMERCIAL USE.

Finally, the Commission should be wary about any claim to ban commercial operations on certain bands of spectrum. Any such approach risks stifling innovation based on absolutist, out-of-step thinking. Here, it is unreasonable to withdraw flexible use rights.

The Petition asserts that "opening DSRC to commercial applications … needlessly creates exploitable vulnerabilities,"[57] but it provides no assessment of risk level. Instead, it takes a rigid approach that "[t]he most secure system is the system that is totally disconnected from all other systems and devices, which avoids adding the complexity of cooperation between entities outside the control of the system operator and reduces the points of entry into the system."[58] It offers no support from security researchers or experts.

The Petition's ask to disconnect DSRC technology from commercial uses runs counter to today's networked and intermingled reality.[59] Perhaps most relevant, the First Responder Network Authority ("FirstNet"), the nationwide broadband interoperable public safety network, will incorporate both public safety and commercial use of its spectrum.[60] FirstNet will do so because Congress believes that public safety and commercial uses can co-exist without risking critical and potentially life-saving communications and data applications.[61] Likewise, federal spectrum users, including the Department of Defense ("DOD"), are exploring use of commercial and other non-federal spectrum bands.[62] The DOD and other federal users do so because they

---

[57] Petition at 12.

[58] *Id.* at 13.

[59] In practice, it also represents a top-down cybersecurity mandate in conflict with the Administration's preferred risk management and self-regulatory approach to cybersecurity.

[60] *See* FirstNet, *Guiding Principles,* http://www.firstnet.gov/about/guiding-principles (last accessed Aug. 24, 2016).

[61] *See id.* ("When Congress created FirstNet, $7 billion was allocated to build the network. The law directed FirstNet to explore the use of *existing … commercial assets* as a way to keep costs down.") (emphasis added).

[62] *See, e.g.,* Commerce Spectrum Mgmt. Advisory Comm., Subcommittee on Federal Access to Non-Federal Bands Recommendations (July 8, 2016), https://www.ntia.doc.gov/files/ntia/publications/federal_access_to_non-federal_bands_sc_report_august_1.pdf; John Eggerton, *Broadcasters, DoD Strike Deal on Sharing BAS Band*, Broadcasting & Cable, Nov. 25, 2013,

believe spectrum can be shared without necessarily compromising the security and viability of their operations.

When the DSRC rules were adopted, the Commission concluded that the record did not provide a technical basis for excluding commercial use, specifically CMRS, as long as its operation met the DSRC service rules.[63] Nothing has changed, and the Petition's contention is unfounded.[64]

Moreover, the prohibition of commercial use would stifle societally beneficial uses of DSRC spectrum for uses including toll collection, traffic management, and congestion mitigation. As NHTSA has indicated, "mobility, weather, and environment applications will benefit from vehicles storing certain limited types of data and, possibly, transmitting and receiving information over multiple communication media, such as DSRC and cellular."[65] An overbroad restriction on the use of DSRC, however, could inhibit the use of DSRC for such beneficial applications, including those under development today and those that may be discovered tomorrow.

---

http://www.broadcastingcable.com/news/washington/broadcasters-dod-strike-deal-sharing-bas-band/125322.

[63] *See Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band)*, Report and Order, 19 FCC Rcd 2458, 2482 ¶ 49 (2004) ("[W]e find that the record does not provide a technical basis for excluding CMRS as a definition matter. Thus, provided that a CMRS operation meets all DSRC service rules, such operation is consistent with our allocation.").

[64] In fact, belying their claim that additional uses of a given communications technology risk harming other important uses of such technology, one of the Petitioners has indicated that more commonly used technologies, including Bluetooth and Wi-Fi, can be used as crash-avoidance technologies instead of DSRC, as such technologies "offer applications comparable to DSRC, but by leveraging wireless connections and devices (e.g., smartphones) that are already ubiquitous for other purposes – and carried by drivers and pedestrians alike." New America Open Technology Institute, *Spectrum Silos to Gigabit Wi-Fi: Sharing the 5.9 GHz 'Car Band'*, at 16 (Jan. 2016), https://static.newamerica.org/attachments/12279-spectrum-silos-to-gigabit-wi-fi/OTI_5.9ghz_web.5de7495517f3416cae27fe811f0f985b.pdf.

[65] *NHTSA V2V Report* at 13.

CONCLUSION

For the reasons described herein, the Commission should reject the Petition and refrain from initiating a new rulemaking regarding cybersecurity, privacy, and commercial use of the DSRC service.

Respectfully submitted,

/s/Thomas C. Power/

Thomas C. Power
Senior Vice President and General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

Jackie McCarthy
Director, Regulatory Affairs

CTIA
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 7885-0081

August 24, 2016